Quantum Information and Computing-Multiple Qubit States and Quantum Gates

Dipan Kumar Ghosh
Department of Physics
Indian Institute of Technology Bombay
Powai, Mumbai 400076

March 16, 2017

Introduction

1 Introduction

We have, in the earlier lectures dealt with qubit, the smallest unit of quantum information. It was pointed out that unlike the classical bits, the qubits can be in a linear superposition of the basis states which provides quantum computation with the power of inherent parallelism. In this lecture, we will extend the concept of a single quit to the case of multi-qubits.

2 Composite Systems:

Consider a composite system consisting of two sub-systems A and B. Let the Hilbert space of A be $\mathcal{H}_A$ and that of B be $\mathcal{H}_B$. The space of the composite system is $\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_{AB}$. Suppose $\{\mid \alpha\rangle_A\}$ be a basis in $\mathcal{H}_A$ and $\{\mid \beta\rangle_B\}$ a basis for $\mathcal{H}_B$. We define the basis of $\mathcal{H}_{AB}$ to be the composite set $\mid \alpha, \beta\rangle_{AB}$. The orthonormality relationship for the basis is

$$_{AB}\langle\alpha', \beta' \mid \alpha, \beta\rangle_{AB} = \delta_{\alpha,\alpha'}\delta_{\beta,\beta'}$$

We define an operator in this composite space as $M_A \otimes N_B$ which acting on a state of the composite system

$$M_A \otimes N_B \mid \psi, \varphi\rangle_{AB} = M_A \mid \psi\rangle_A \otimes N_B \mid \varphi\rangle = \sum (M_A)_{\psi,\alpha} \mid \alpha\rangle (N_B)_{\varphi,\beta} \mid \beta\rangle$$

Let us look at two qubit system. The corresponding cbits are 00, 01, 10 and 11. The quantum states for two qubits is

$$\mid \psi\rangle = \alpha_{00} \mid 00\rangle + \alpha_{01} \mid 01\rangle + \alpha_{10} \mid 10\rangle + \alpha_{11} \mid 11\rangle$$

subject to $\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2 + \mid \alpha_{10} \mid^2 \mid \alpha_{11} \mid^2 = 1$.

Suppose we measure the first qubit and get 0 (with probability $\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2$). The post measurement state is

$$\mid \psi' \rangle = \frac{\alpha_{00} \mid 00\rangle + \alpha_{01} \mid 01\rangle}{\sqrt{\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2}}$$

Note that not all two qubit states can be written as a product of single qubit states. A particularly important set of such stares is known as **Bell states** which are given by

$$\begin{aligned}
\mid \psi_+ \rangle &= \frac{\mid 01\rangle + \mid 10\rangle}{\sqrt{2}} \\
\mid \psi_- \rangle &= \frac{\mid 01\rangle - \mid 10\rangle}{\sqrt{2}} \\
\mid \phi_+ \rangle &= \frac{\mid 00\rangle + \mid 11\rangle}{\sqrt{2}} \\
\mid \psi_- \rangle &= \frac{\mid 00\rangle - \mid 11\rangle}{\sqrt{2}}
\end{aligned}$$

Suppose we measure the first qubit of one of the members of the above states, say, $\mid \psi_+ \rangle$. If we get 0 as a result of the measurement, it could only have come from the component $\mid 01\rangle$, which would be the normalized post-measurement state of the system. However, note that as a result of this measurement, even though we did not measure it, the state of the second qubit also got determined to be $\mid 1\rangle$. This shows that the measurement outcomes are correlated. The states in the example of Bell basis given above as then said to be **entangled**.

3 Matrix Basis in the space of two qubits

We have seen that in the Hilbert space $\mathbb{C}^2$ for one qubits, we could define a column vector representation for the states. One of the possible basis in this space was the **computational basis** : $\mid 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mid 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. We may use this to define a basis for the higher dimension as well. For instance, the computational basis for the two qubit

states are obtained as the matrix direct product of the one qubit basis states as follows:

$$| 00\rangle =| 0\rangle\otimes | 0\rangle = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$| 01\rangle =| 0\rangle\otimes | 1\rangle = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$| 10\rangle =| 1\rangle\otimes | 0\rangle = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$| 11\rangle =| 1\rangle\otimes | 1\rangle = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

One can generalize this to the case of n qubits and define an n-qubit state as

$$| a_0, a_1, \ldots, a_{n-1}\rangle =| a_1\rangle\otimes | a_2\rangle \ldots | a_n\rangle$$

where each of the components a_i takes value 0 or 1. Thus such a state can be simultaneously in a linear combination of 2^n states and contains this much amount of information. However, we will see later that much of this information remain hidden and a measurement can only reveal n qubits of information.

Measurement is a very important component of quantum information, because, unlike the classical, the results in this case are probabilistic. We often talk about measurement in computational basis which simply means preparing our measurement apparatus in the basis described above. However, a basis in the Hilbert space need not only be computational. Any set of vectors in terms of which one can express an arbitrary state forms a basis as well. To illustrate, in $\mathbb{C}^2$ the states $| 0\rangle$ and $| 1\rangle$ form the computational basis. However, if we have a general state $\alpha 0 + \beta 1$, a repeated measurement in this basis may give us information about $| \alpha |$ and $| \beta |$ but not about any relative phase between the two complex coefficients. If, however, we made a measurement of this state in what we called as the *diagonal basis* which consists of taking the basis vectors as $\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\}$, it may reveal some information about the relative phase as well.

4 Single Qubit Gates

Having discussed the essential logic elements qubits, which correspond to the classical bits, we now discuss the logic gates which acts on a quantum state to give another state in the same Hilbert space. The situation is very similar to the case of classical computing where we only need to construct some universal logic gates (e.g. NOR and NAND) in terms of which any boolean function may be expressed. In quantum computer as well, we will need only a few elementary gates. There is one major difference between the quantum and classical case. In quantum world, the states develop unitarily (except at the time of measurement) and therefore, the gates must perform their operations **unitarily** and **reversibly**. (In classical computation as well, one of the gates, viz, the NOT gate is reversible but not all are). Like in a classical computers we would have here registers for input and output, which now has the capability of storing linear combination of states. In performing computation, we need some additional registers which will be termed as **ancilla**. The unitary operations preserve the norm of a quantum state. We may recall that the single qubit states have a geometric representation on a unit sphere called Bloch sphere. Since the unitary operations preserve the length of a vector, they would take one point on the Bloch sphere to another point on the same sphere, which means the operations correspond to rigid rotation and reflection on the sphere.
In terms of the matrix representation, the situation is as follows. Since the operations will be performed on a state $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ resulting in another state $\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix}$, the operators which act on the states are represented as a 2×2 matrix. We will show in the following that a 2×2 matrix can be represented in the form

$$U = e^{i\alpha}\exp\left(-i\theta\hat{n}\cdot\vec{\sigma}/2\right)$$

where α and θ are real numbers, $\hat{n}$ is a unit vector in space and $\vec{\sigma}$ is Pauli vector having the components

$$\sigma_x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$
$$\sigma_y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$$
$$\sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

To prove this, we proceed as follows. Let the matrix be

$$U = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

where a, b, c, d are, in general complex. It may be noted that any 2×2 matrix may be written as a linear combination of the identity matrix I and the Pauli matrices given

above. Writing the matrix as

$$U = u_0 I + u_1 \sigma_x + u_2 \sigma_y + u_3 \sigma_z$$

we have,

$$\begin{aligned} UU^\dagger &= (\mid u_0 \mid^2 + \mid u_1 \mid^2 + \mid u_2 \mid^2 + \mid u_3 \mid^2) I + [u_0 u_1^* + u_0^* u_1 + i(u_2 u_3^* - u_3 u_2^*)]\, \sigma_x \\ &= [u_0 u_2^* + u_0^* u_2 + i(u_3 u_1^* - u_1 u_3^*)]\, \sigma_y + [u_0 u_3^* + u_0^* u_3 + i(u_1 u_2^* - u_2 u_1^*)]\, \sigma_z \end{aligned}$$

where we have used the relations $\sigma_i^2 = I$ and $\sigma_i \sigma_j = i\epsilon_{ijk}\sigma_k$. Since this to be an identity matrix, we must have the following:

$$\begin{aligned} \mid u_0 \mid^2 + \mid u_1 \mid^2 + \mid u_2 \mid^2 + \mid u_3 \mid^2 &= 1 \\ u_0 u_1^* + u_0^* u_1 + i(u_2 u_3^* - u_3 u_2^*) &= 0 \\ u_0 u_2^* + u_0^* u_2 + i(u_3 u_1^* - u_1 u_3^*) &= 0 \\ u_0 u_3^* + u_0^* u_3 + i(u_1 u_2^* - u_2 u_1^*) &= 0 \end{aligned}$$

These equations may be satisfied if we choose

$$\begin{aligned} u_0 &= e^{i\alpha} \cos(\theta/2) \\ u_1 &= -ie^{i\alpha} \sin(\theta/2) n_x \\ u_2 &= -ie^{i\alpha} \sin(\theta/2) n_y \\ u_3 &= -ie^{i\alpha} \sin(\theta/2) n_z \end{aligned}$$

where $n_x^2 + n_y^2 + n_z^2 = 1$.

5 Single Qubit Gates

We had seen in the last lecture that the classical NOT gate is a reversible gate. Its quantum counterpart which maps the state $\mid 0\rangle$ to $\mid 1\rangle$ and vice versa is provided by Pauli's σ_x matrix. The gate is called an X-gate, whose matrix representation is given by

$$X : \ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

NOT gate is the only single qubit gate possible in classical computing. However, because of the nature of the quantum states, there are other possibilities existing here. One such is a phase gate, which acting on the state $\mid 0\rangle$ leaves it unchanged but acting on the state $\mid 1\rangle$ gives $-\mid 1\rangle$

$$\text{Phase Gate} : \quad \mid 0\rangle \rightarrow \mid 0\rangle \qquad \mid 1\rangle \rightarrow - \mid 1\rangle$$

The matrix representation of the corresponding operator is given by Pauli matrix σ_z and the gate is known as the Z-gate

$$Z: \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

In general, one could talk about a selective phase operation for the single qubit states, which selectively gives a phase of φ to the qubit $\mid 1\rangle$ while leaving $\mid 0\rangle$ unchanged

$$\mid 0\rangle \rightarrow \mid 0\rangle \qquad \mid 1\rangle \rightarrow e^{i\varphi} \mid 1\rangle$$

the corresponding matrix representation being

$$P(\varphi) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

It is easily seen that the Z-gate is a special case of the above with $\varphi = \pi$. There are a few other special phase gates which are important in quantum computing, one of them being T-gate with corresponds to $\varphi = \pi/4$ having a matrix representation

$$\text{T Gate} := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Interestingly, this gate is also known as $\pi/8$ gate, the reason for this nomenclature is due to the fact that if one takes away an overall phase factor of $e^{i\pi/8}$, the structure of the gate becomes

$$\frac{\pi}{8} \ \text{Gate} := \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

Other possibilities include a rotation in a plane. For instance, the operator for rotation about the z-axis is given by the rotation matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

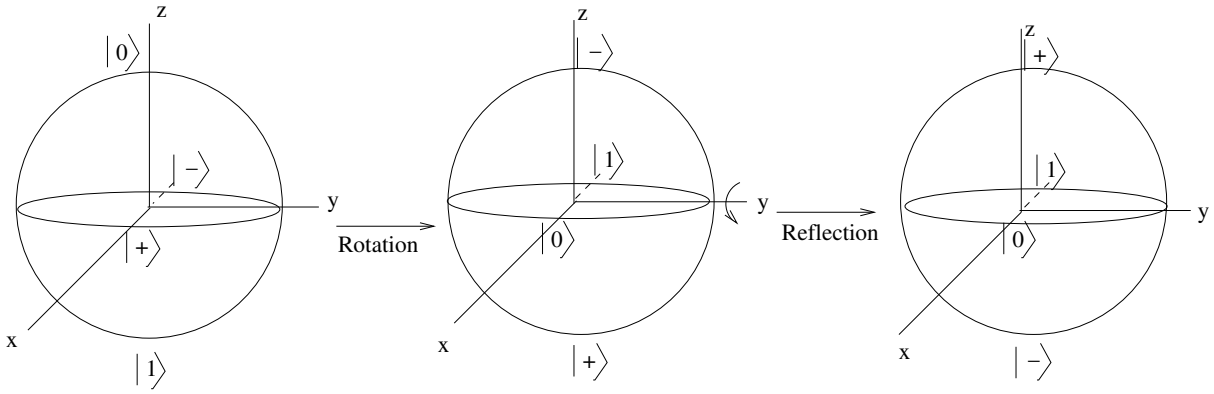
5.1 Hadamard Gate

One of the most important single qubit gate is a Hadamard Gate, because this is a gate which acting on qubit $\mid 0\rangle$ or $\mid 1\rangle$ would mix them up:

$$\mid 0\rangle \rightarrow \mid +\rangle = \frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}}; \quad \mid 1\rangle \rightarrow \mid -\rangle = \frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$$

We have seen that every state has a distinct position on a Bloch sphere. The effect of Hadamard gate on the single qubit state is a rotation by $\pi/2$ about the y-axis followed by a reflection in the equatorial plane. The figure shown illustrates this. It may be remembered that in a rotation, the sense of rotation is taken to be counterclockwise. Thus when a rotation about y-axis by $\pi/2$ is given, the states $\mid 0\rangle$ and $\mid 1\rangle$ come respectively to the

position of $|+\rangle$ and $|-\rangle$ respectively, as is required by Hadamard gate. However, when one applies Hadamard gate on the state $|+\rangle$, it should give the state $|0\rangle$ and likewise the state $|-\rangle$ should give the $|1\rangle$. However, the rotation above interchanged these two positions. A reflection in the equatorial plane would give the correct positions for these two without affecting the positions of the states in that plane.

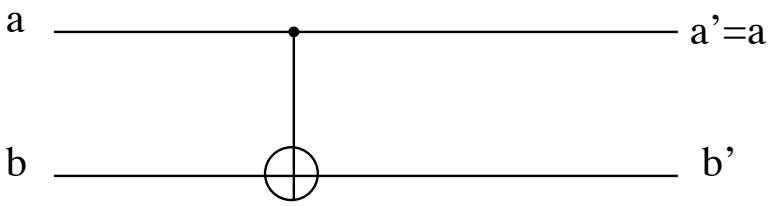


The matrix representation of the Hadamard gate is seen to be

$$\text{H Gate} := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

5.2 Two Qubit Gates

We have seen that in classical computing NAND gate acts as a universal gate in the sense that any boolean operation may be performed using NAND gates alone. Likewise, all quantum operations may be performed to arbitrary degree of precision by using a subset of single qubic gates and a two qubit gate alone. The two qubic gate which is a member of the universal gate set is the **Controlled NOT** or in short **CNOT** gate. This gate takes two inputs, a control and a target. When the control bit is 0, the target bit remains unchanged but when the control bit is 1, the target is flipped.



Thus the effect of control gate is as follows:

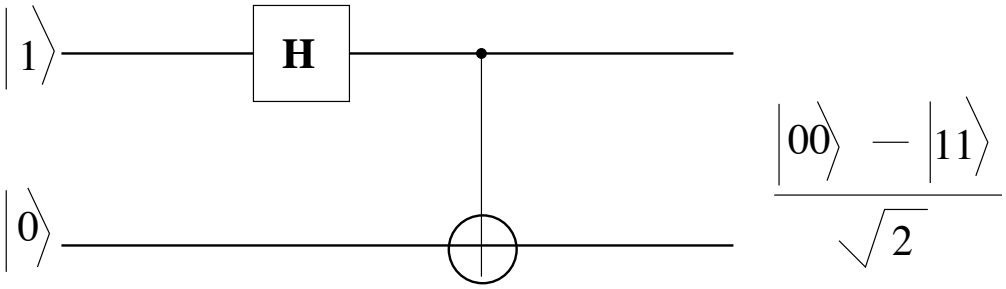
$$|0\rangle \otimes |b\rangle \rightarrow |0\rangle \otimes |b\rangle$$
$$|1\rangle \otimes |b\rangle \rightarrow |0\rangle \otimes |\tilde{b}\rangle$$

where $\tilde{b}$ stands for complement of b. With the computational basis as the basis for the

two qubits, the matrix representation for the CNOT gate is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

We have earlier talked about the Bell basis. We may design a quantum circuit using a Hadamard gate and a CNOT gate.



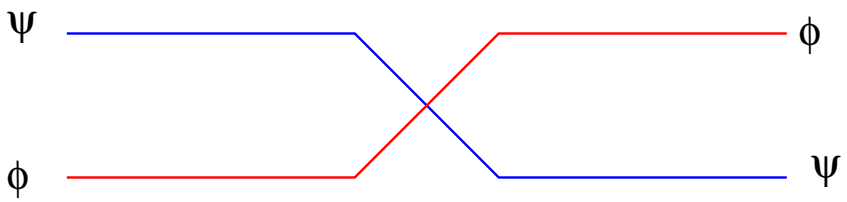
Note that CNOT gate provides the entanglement required for the Bell state. Starting with $\mid 1\rangle \otimes \mid 0\rangle$, we subject first state to a Hadamard gate. This makes the control bit to $\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$, so that the two qubit state is given by $\frac{1}{\sqrt{2}}(\mid 00\rangle - \mid 10\rangle)$, which is still factorable and hence are not entangled. However, when the CNOT gate is applied to these two states, one gets a Bell state $\frac{1}{\sqrt{2}}(\mid 00\rangle - \mid 11\rangle)$ because while the first term is unchanged, in the second term, the control bit being 1, the target which was 0 got flipped. A two qubit gate which is useful is a SWAP gate which interchanges two states :

$$U_S \mid \psi\rangle \otimes \mid \phi\rangle \rightarrow \mid \phi\rangle \otimes \mid \psi\rangle$$

The operator representation of this gate is

$$U_S = \mid 00\rangle\langle 00 \mid + \mid 01\rangle\langle 10 \mid + \mid 10\rangle\langle 01 \mid + \mid 11\rangle\langle 11 \mid$$

The schematic diagram of the gate is as follows:



6 Three Qubit Gates

One can define some three qubit gates as well, though they are strictly not required. There is a gate called **Controlled-Controlled NOT** or **CCNOT** gate, which has two

qubits as the control and a third qubit as the target. In this case, the target bit is flipped only when both the control bits are equal to 1. This gate is reversible and can simulate all classic gates. However, this is not used in practice in the classical situation because of accumulation of garbage. The gate is also known as **Toffoli Gate**. The representation of a CCNOT gate is as follows:

In the diagram the symbol $\oplus$ stands for addition modulo 2 operation. The operator representation for this gate is

$$U_{CCNOT} = (\mid 00\rangle\langle 00 \mid + \mid 01\rangle\langle 01 \mid + \mid 10\rangle\langle 10 \mid) \otimes I + \mid 11\rangle\langle 11 \mid \otimes X$$

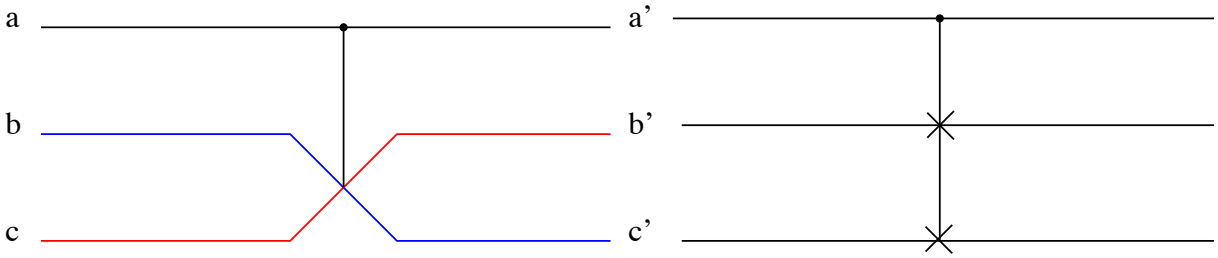
where the operators act on the three qubits in the order in which the above relation is written, i.e. only if the AND operation on the targets yield 1, then only the target bit is flipped. The truth table of the Toffoli gate is as follows

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

The matrix representation of the CCNOT gate is given by an 8×8 matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Yet another three qubit gate that is useful is controlled Swap**CSWAP** gate, which interchanges two target bits if the control bit is 1. There are two equivalent diagrammatic representation of this gate which are shown below:



This gate is also known as **Fredkin Gate**. The Truth table of the Fredkin gate is as follows:

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1